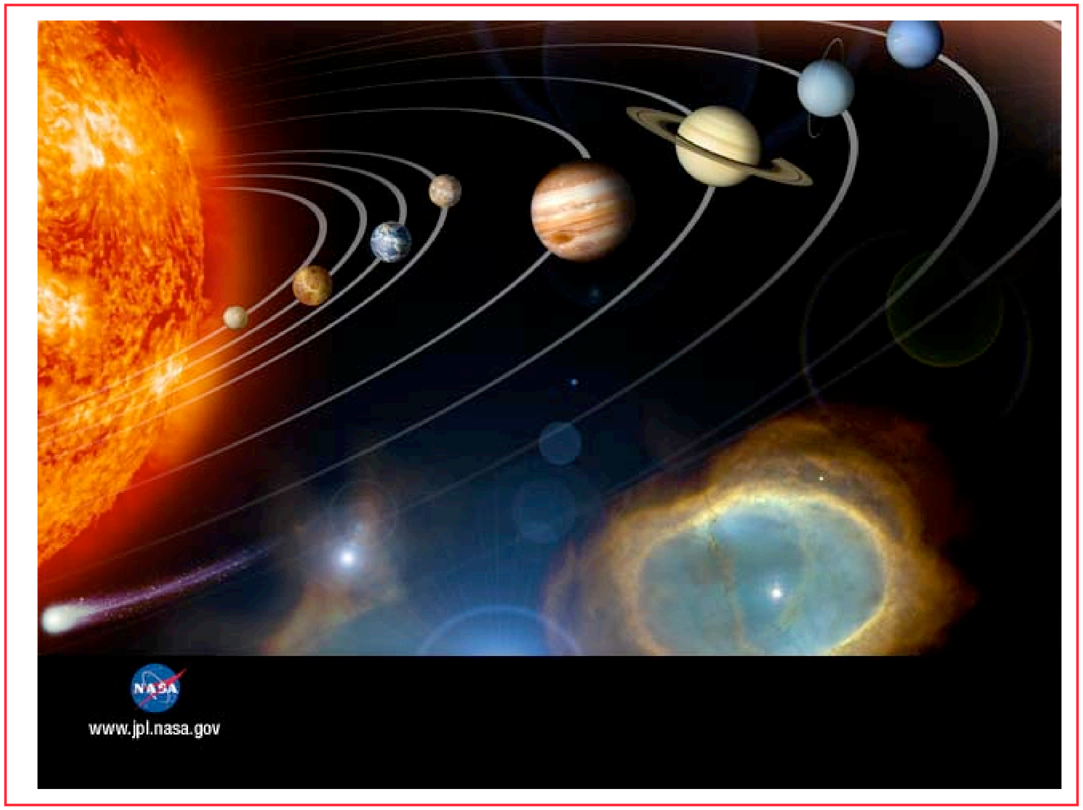
ISHEM Forum

# Robotic Spacecraft:

## "Fault Protection Techniques in JPL Spacecraft"



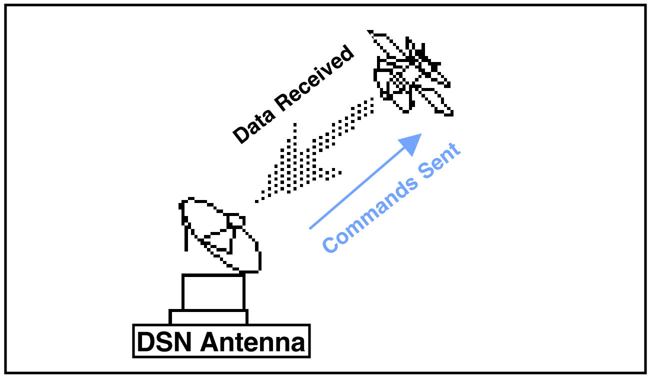
**Paula S. Morgan, (818)393-1092**
NASA – Jet Propulsion Laboratory

# Agenda

- **Definition of JPL Spacecraft Missions**
- **Health & Safety Concerns for Robotic Missions**
- **Standard JPL Fault Protection Techniques**
  - Approach
  - Application
  - Examples
- **Conclusions**

# Definition of JPL Spacecraft Missions

- **Once JPL Spacecraft are ferried out of Earth's gravity well, it will either enter Earth's orbit or proceed out into deep space**
  - A "Ground-Based Operations Team" will stay in contact with the spacecraft via NASA's Deep Space Network (DSN) antenna system
    - Instructions are sent to spacecraft through "uplink" commands
    - Spacecraft information is received through its "downlink" telemetry stream of all it encounters throughout its mission



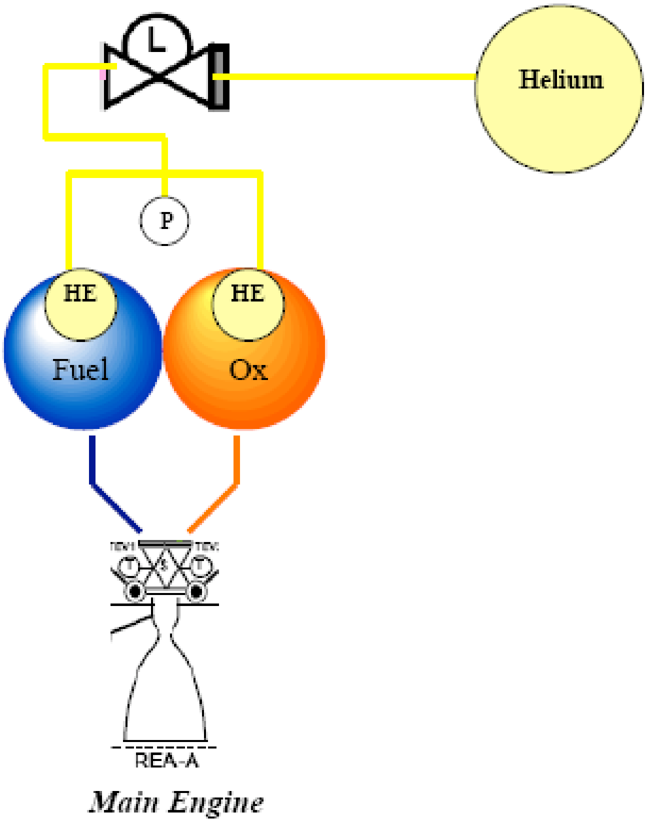
  - JPL's interplanetary spacecraft mission objectives typically consist of
    - Orbiting or flying around an object, moon or planet
    - Landing the spacecraft or its probe on an object it is encountering
    - Collecting scientific data  through the spacecraft's suite of instruments
  - Resolving problems experienced by the spacecraft is the responsibility of the Ground-Based Operations Team

# Health & Safety Concerns for Robotic Missions

- **Many fault sources affect subsystems & instrument health during the Spacecraft's mission:**
  - Temperature excursions from Sun exposure & cold of deep space
    - Surfaces can superheat when exposed to the Sun while surfaces in the shadow can fall to extremely low temperatures
      - Instruments can fall out of operating limits since many devices will only operate within a narrow range of temperatures
      - Material stresses from thermal expansion-contraction; uneven heating can lead to warpage, camera distortion, or breakage of components
      - Thermal state of spacecraft's gas or liquid fuel must be maintained to prevent freezing due to deep space exposure, rendering the propellant unusable
        - A non-maneuverable spacecraft will eventually become misaligned with Earth so that no signals can be sent or received by spacecraft
        - Interior heat buildup can occur from spacecraft's own systems; these substances are sometimes circulated for interior cooling
  - Errors due to Human Interaction
    - Device "latent failures" from electro-static discharge events during the manufacturing process (device useless or partially useless)
    - Uplink command errors (in "command sequences" such as Earth tracking, monitoring celestial references for attitude calibration, science data collection, etc.)
      - Fault Example: Accidentally turning off a radio transmitter or receiving device will lead to an inability to communicate with the spacecraft
  - Spacecraft component faults: device failures, power loss, oversubscription of power resource, fuel tank over-pressure or under-pressure levels, etc.

# Health & Safety Concerns for Robotic Missions – Cont.

- **“Limiting Factors”: Earth-to-Spacecraft transmission “Lag Time”**
  - Missions designed for great Earth-to-Spacecraft distances experience an ever-increasing transmit/receive “lag time”
    - Radio waves travel at the speed of light making Spacecraft-Earth transactions almost instantaneous near Earth, but at the outer planets, a radio signal can take hours
    - Example: Lag time for Cassini Spacecraft orbiting Saturn-Titan system = 1hr 20min
  - Lag time is a deterrent to fault recovery when spacecraft are sent out great distances
    - For some faults, spacecraft cannot respond to Ground commands in time to preclude a catastrophic failure
    - Example: Helium latch valve closure failure during tank pressurization task; increasing tank pressures can rise substantially in a short period of time causing tank rupture (mission failure)
  - Also, faults in the presence of crucial “one time events” such as planet/moon encounters can lead to loss of mission objectives



# Health & Safety Concerns for Robotic Missions – Cont.

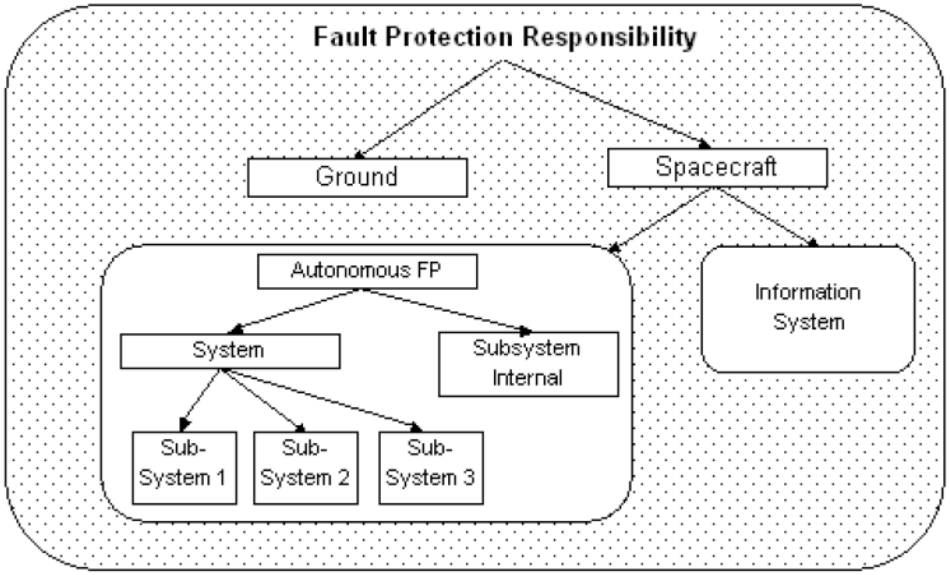
- **As spacecraft design becomes more complex, fault diagnosis & resolution becomes a more difficult, time-consuming task**
  - A plethora of fault possibilities can exist for a complex system
  - To determine fault causes and resolution actions, a huge volume of data must be collected from the Spacecraft's telemetry stream

- **To address these health & safety issues, Fault Protection (FP) Techniques are implemented into the spacecraft through:**
  - Functional redundancy
  - Redundant hardware
  - On-board autonomous FP routines within flight software -
    - To continuously monitor systems
    - To respond to anomalous conditions
      - Invoke fault responses which contain "pre-programmed instructions" to place spacecraft in a safe, predictable state
      - Perform redundant unit swaps when required

- **Fault resolution responsibility is allocated to both Spacecraft & Ground Team**
  - On-board Spacecraft FP is only implemented when:
    - Ground commanded response is not feasible or practical
    - Action is required within a pre-defined period of time of detecting a failure

## Standard JPL Fault Protection Techniques:  Approach

- **FP responsibility is allocated to both Spacecraft & Ground Team**
  - Spacecraft must deliver sufficient information on system health to facilitate fault recovery by the Ground Team or Spacecraft's Automated FP



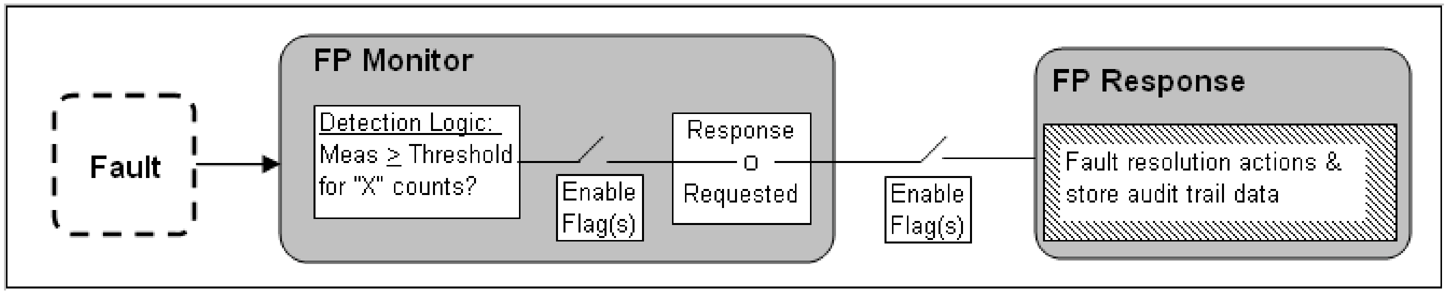
  - Spacecraft Autonomous FP is divided into two applications:
    - "Subsystem Internal FP (SIFP)"
      - If the subsystem can recover itself without affecting the functionality or operation of another subsystem
      - FP actions are localized to subsystem components
    - "System Fault Protection (SFP)"
      - Addresses those faults which affect the entire Spacecraft

# Standard JPL Fault Protection Techniques:  Approach – Cont.

- **Spacecraft autonomous FP is designed with the following priorities:**
    - Protect critical spacecraft functionality
    - Protect spacecraft performance & consumables (i.e. fuel)
    - Minimize disruptions to normal operations
    - Simplify Ground Team recovery response

- **And ensures:**
    - Spacecraft is placed in a safe, predictable state
    - Telemetry information is sufficient to analyze & reconstruct FP actions
    - Faults detected during critical events:  event success has priority; spacecraft safety has lower priority until event is completed

- **FP is structured as “Monitors” & “Responses”; can be enabled / disabled during the mission**
    - Monitors evaluate measurements against predefined “threshold” value to determine if fault condition exists; may count consecutive occurrences before taking action for a fault
        - To ensure transient conditions do not trigger a response
        - To satisfy hardware turn-on constraints
        - To allow other higher priority FP algorithms to execute first
    - Responses initiate actions to place the spacecraft in a safe, predictable state



# Standard JPL Fault Protection Techniques: Application

- **Although each JPL spacecraft is unique in its configuration & mission objectives, FP techniques may be implemented in a generic manner**
  - Some spacecraft designs are simple enough to warrant only minimal FP meant to address any fault condition
  - Other spacecraft designs are very complex, have long mission durations, and must maintain a system with numerous error possibilities
  - But all spacecraft share common systems which require a similar approach in FP design
    - Maintaining communication with Earth
    - Maintaining power level
    - Controlling internal & external environmental influences

## Standard FP Techniques

1. The **"Safe-Mode" Fault Response**: Most spacecraft rely on a "general-purpose" fault response which typically configures the spacecraft to a lower power state:
   - Powers off all non-essential devices
   - Thermally safe attitude commanded
   - Establishes an uplink & downlink with Earth
   - Reconfigures to "low-gain" antenna
   - Terminates currently executing command sequence

- This response configures the spacecraft to a safe, predictable state which can be maintained for a limited period of time, so that the Operations Team may evaluate fault causes, determine their impact on the spacecraft, and determine fault resolution actions

# Standard JPL Fault Protection Techniques: Application – Cont

## Standard FP Techniques – Cont.

2. The **"Under-Voltage" Fault Response:** Recovery from a system-wide loss of power

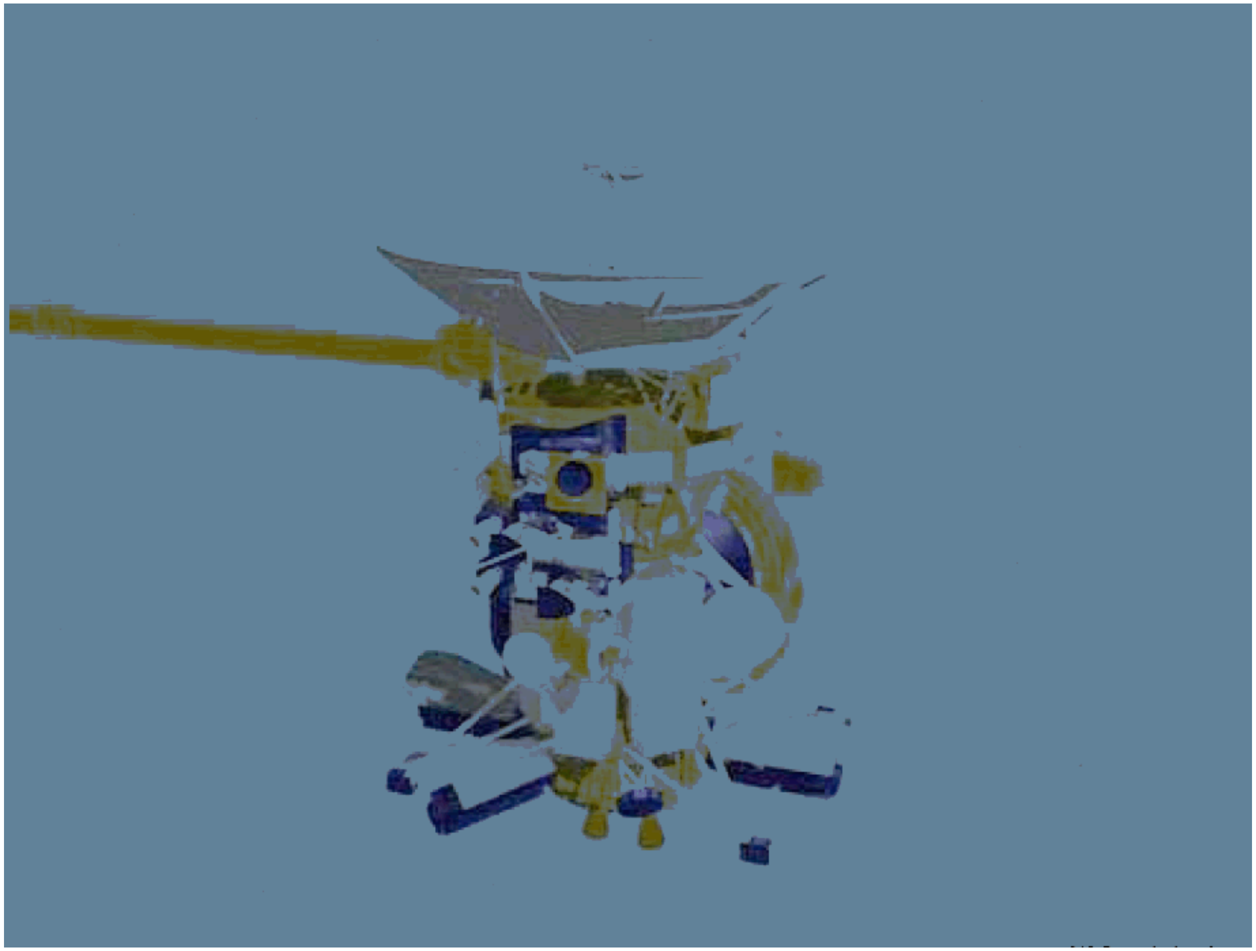
   - Fault causes: oversubscribing power available, short in power system, bus overload
   - For this type of fault, not even Safe Mode response will run since the main computer will lose power (loss of mission)
   - Once FP senses power drop, response will:
     - Isolate defective device (e.g. Radioisotope Thermoelectric Generator (RTG))
     - Shed non-essential loads from communications bus
     - Regain voltage regulation
     - Re-establish essential hardware
   - The quick actions of this response allow computer memories to be maintained throughout the under-voltage event (see example in BU #1)

3. The **"Command Loss Response":** Recovery from a "loss of spacecraft signal" condition

   - Covers faults which affect the Ground Team's ability to communicate with the spacecraft
   - Fault causes: spacecraft hardware failures, RF interferences, erroneous attitude pointing errors, uplink command errors, environmental interferences, antenna failures
   - The configuration of this response depends upon the particular hardware installed on the spacecraft
   - Goal of response is to reconfigure the spacecraft's state until the uplink is restored by:
     - Performing hardware swaps
     - Re-commanding spacecraft attitude
     - Performing antenna swaps
   - This is typically an "endless-loop" response

## Standard JPL Fault Protection Techniques: Example

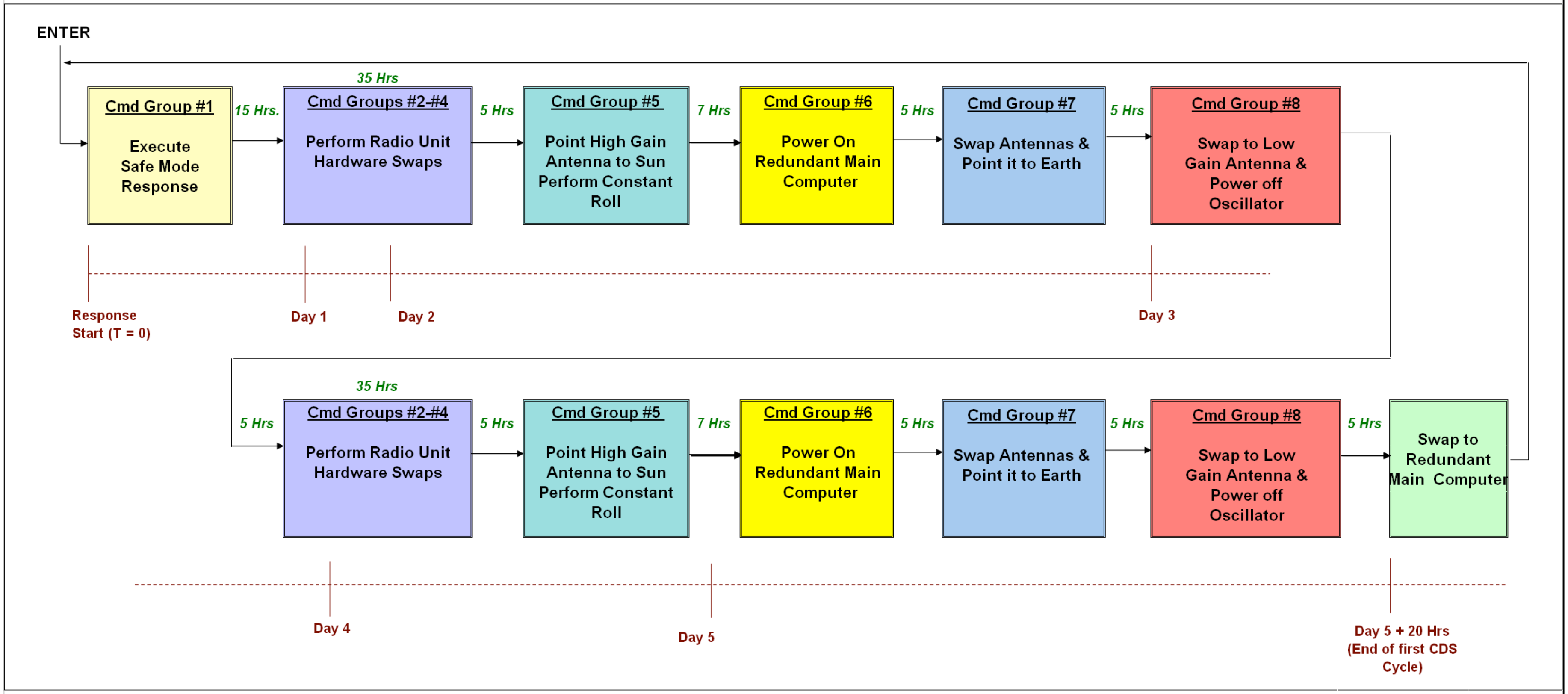
### Example: Cassini Spacecraft's Command Loss Response



- The Cassini spacecraft contains redundant main computers, attitude control computers, radio devices, and 3 antennas

# Standard JPL Fault Protection Techniques: Example - Cont.

- **Example: Cassini Spacecraft "Command Loss Response"**
  - "Loss of spacecraft signal" condition is determined by a timer aboard the spacecraft
    - Decrements continuously; reset back to default value each time a command is received
    - This is the monitor's "persistence filter"; response executes when timer reaches "0"
      - Response consists of "Command Groups"; "Command Pauses" after each group allows Ground Team to attempt re-acquisition with newly commanded configuration
      - Once uplink is re-established, response is terminated, timer is reset (leaving the spacecraft on the successfully commanded configuration)



ENTER

Cmd Group #1: Execute Safe Mode Response

15 Hrs.

35 Hrs

Cmd Groups #2-#4: Perform Radio Unit Hardware Swaps

5 Hrs

Cmd Group #5: Point High Gain Antenna to Sun Perform Constant Roll

7 Hrs

Cmd Group #6: Power On Redundant Main Computer

5 Hrs

Cmd Group #7: Swap Antennas & Point it to Earth

5 Hrs

Cmd Group #8: Swap to Low Gain Antenna & Power off Oscillator

Response Start (T = 0)

Day 1

Day 2

Day 3

5 Hrs

35 Hrs

Cmd Groups #2-#4: Perform Radio Unit Hardware Swaps

5 Hrs

Cmd Group #5: Point High Gain Antenna to Sun Perform Constant Roll

7 Hrs

Cmd Group #6: Power On Redundant Main Computer

5 Hrs

Cmd Group #7: Swap Antennas & Point it to Earth

5 Hrs

Cmd Group #8: Swap to Low Gain Antenna & Power off Oscillator

5 Hrs

Swap to Redundant Main Computer

Day 4

Day 5

Day 5 + 20 Hrs (End of first CDS Cycle)

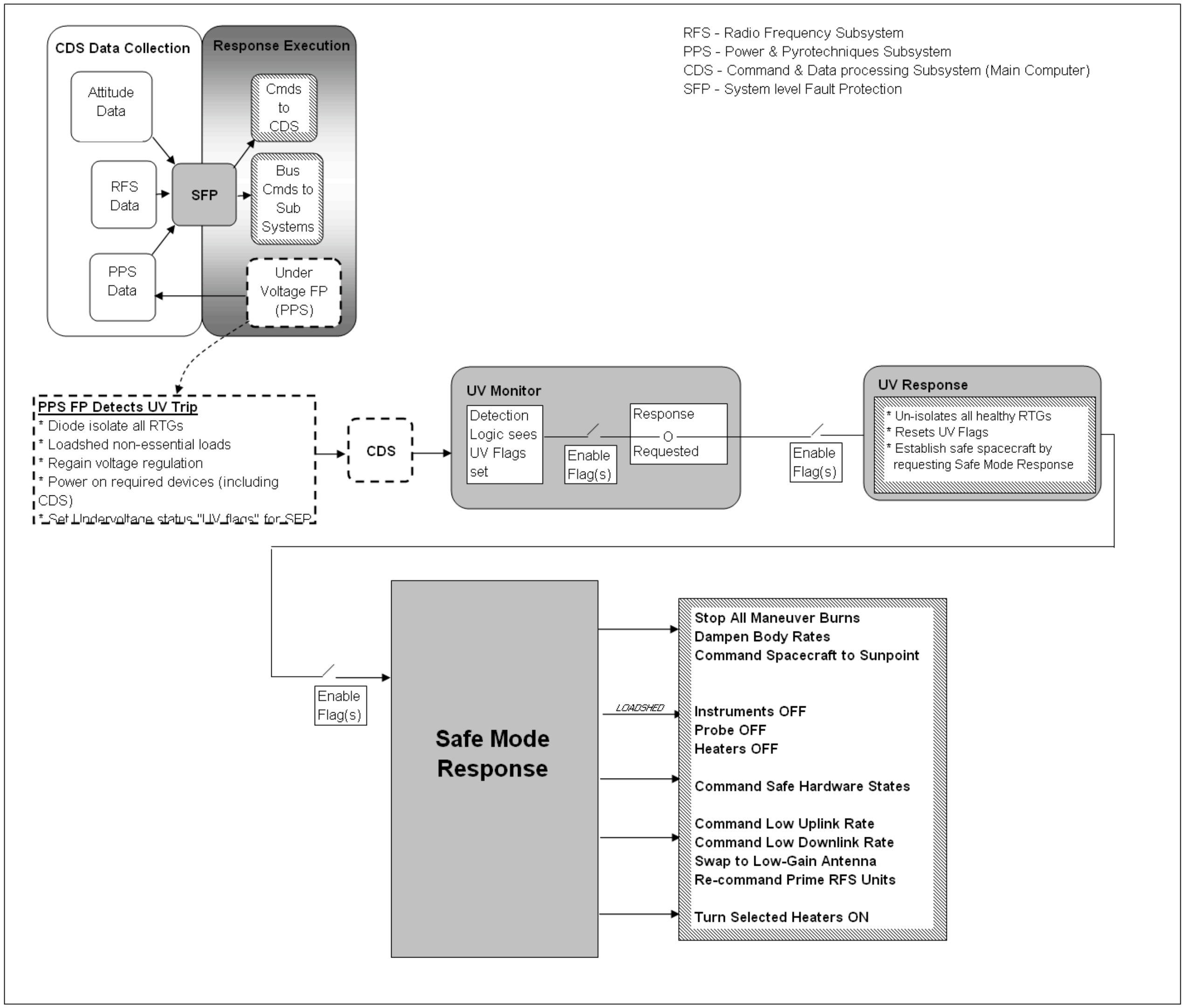
# Conclusions

- **For Spacecraft to function properly without significant risk or degradation during its mission or mission objectives, continuous monitoring of components & subsystems is desirable**
  - Continuous monitoring the spacecraft's telemetry stream by personnel is impractical
  - Communication through the DSN facility is quite costly
- **Hence, the common problems experienced by most spacecraft:**
  - Environmental influences
  - Human error
  - Device failures
  - Fault occurrences in the presence of transmit/receive lag time
  - The large volume of fault possibilities due to spacecraft complexity

  **may be alleviated by implementing autonomous solutions within the spacecraft itself**
- **To monitor, detect, and resolve the faults as they are encountered where possible, so that the spacecraft may preserve its overall health and provide a system with greater diagnostic capabilities**

# Backup Charts

# BU #1: Cassini Spacecraft's Under Voltage FP Actions for Shorted RTG


RFS - Radio Frequency Subsystem
PPS - Power & Pyrotechniques Subsystem
CDS - Command & Data processing Subsystem (Main Computer)
SFP - System level Fault Protection
CDS Data Collection
Attitude Data
RFS Data
PPS Data
SFP
Response Execution
Cmds to CDS
Bus Cmds to Sub Systems
Under Voltage FP (PPS)
PPS FP Detects UV Trip
* Diode isolate all RTGs
* Loadshed non-essential loads
* Regain voltage regulation
* Power on required devices (including CDS)
* Set Undervoltage status "UV flags" for SFP
CDS
UV Monitor
Detection Logic sees UV Flags set
Enable Flag(s)
Response Requested
Enable Flag(s)
UV Response
* Un-isolates all healthy RTGs
* Resets UV Flags
* Establish safe spacecraft by requesting Safe Mode Response
Enable Flag(s)
Safe Mode Response
LOADSHED
Stop All Maneuver Burns
Dampen Body Rates
Command Spacecraft to Sunpoint
Instruments OFF
Probe OFF
Heaters OFF
Command Safe Hardware States
Command Low Uplink Rate
Command Low Downlink Rate
Swap to Low-Gain Antenna
Re-command Prime RFS Units
Turn Selected Heaters ON

**Cassini Spacecraft's Under-Voltage FP / Safe Mode FP Response:** In this example, a Radioisotope Thermoelectric Generator (RTG) power unit (one of three on the spacecraft), has shorted out. The Power Subsystem (PPS) FP senses a power drop below the predefined threshold for the duration of the persistence filter. The first action taken by the PPS FP is to diode isolate All three RTGs, turn off (loadshed) all spacecraft non-essential loads, regain the voltage regulation, and turn on all essential hardware. It also sets three "UV Status Flags" to notify SFP that an Under Voltage event has occurred. Once the main processing computer (CDS) becomes operational, it will deliver the status of these UV Status Flags to SFP. SFP's Under Voltage monitor will examine the state of each RTG and if enabled, will request the Under Voltage response. The response un-isolates the correctly operating RTGs, unsets the "UV Status Flag", and establishes a predictable, safe spacecraft state by executing the Safe Mode response.

# BU #2: Standard FP Application in JPL Spacecraft

***Figure (1a) through Figure (1c) show three JPL spacecraft designs with quite different mission objectives, which employ most standard fault protection. Their mission design unique fault protection is also listed.***

*Figure (1a). CloudSat Spacecraft FP Allocation*

**CloudSat:** *Earth Orbiting Satellite*

**Standard FP:** 3 Safe Mode Responses
5 Under-voltage Responses
Memory Scrubber & Bus FP
**Unique FP:** Significant computer & thermal FP

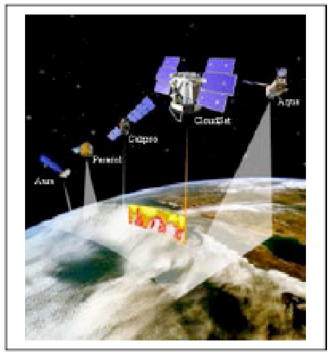


*Figure (1b). Stardust Spacecraft FP Allocation*

**Stardust Spacecraft:** *Inner Solar System; Comet Explorer*
**Standard FP:** 1 Safe Mode Response
1 Under-voltage Response
1 Command Loss Response
Memory Scrubber & Bus FP
**Unique FP:** Some computer & thermal FP

*Figure (1c). Cassini Spacecraft FP Allocation*

**Cassini Spacecraft:** *Outer Solar System; Saturn-Titan Explorer*

**Standard FP:** 1 Safe Mode Response
1 Post-Safe Mode Response
1 Under-voltage Response
1 Command Loss Response
Memory Scrubber & Bus FP
**Unique FP:** Significant command & data processing computer FP, radio unit FP, thermal FP, fuel tank pressure FP, attitude articulation and control computer FP